Policy for Use of Removable Media, Such as USB "Thumb" Drives 11.21.2008

This message is being distributed to all NASA civil service and contractor employees. Point of Contact: Jerry Davis, Office of the Chief Information Officer, 202-358-1401.

There is a government-wide increase in the number of IT security threats originating from removable media which infect systems with malicious code and/or remove sensitive data such as usernames, passwords and encryption keys from user systems.

Removable media typically consists of portable devices that can be used to copy, save, store and/or move data from one system to another. Media devices come in various forms that include, but are not limited to, USB drives, flash drives or cards, read/write CDs, memory cards, external hard drives and Personal Digital Assistant (PDA) storage cards.

While removable media are extensively used for storing and transporting data, some of the characteristics that make them convenient to use also introduce security risks, due in large part to the fact that they are typically unmanaged storage devices.

The United States Computer Emergency Readiness Team (US-CERT) recommends that agencies and organizations implement several best practices with regard to removable media devices to assist in mitigating the associated risks.

The following policy is effective immediately based on these best practices:

NASA Policy:

Do not use personally owned removable media devices in government-owned systems.

Do not use government-owned removable media devices on personal machines or machines that do not belong to your agency, department or organization.

Do not put unknown removable media devices into ANY system.

Keep systems up-to-date with the latest patches and anti-virus signatures.

Cyber Security Tip ST08-001 available at the US-CERT Web site provides more cautionary information on the use of USB drives.

As NASA Chief Information Officer (CIO), I am in the process of updating security policies and am also working with center CIOs on additional measures recommended by US-CERT to mitigate removable media risks, including implementation of Federal Desktop Core Configuration (FDCC) settings.

Your compliance with this policy and implementation of other mitigating measures is imperative for the protection of NASA's information and systems.

We appreciate your diligence on this matter.

Jonathan Q. Pettus
Chief Information Officer